UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

| APPLICATION NO. | FILING DATE | FIRST NAMED INVENTOR | ATTORNEY DOCKET NO. | CONFIRMATION NO. |
|---|---|---|---|---|
| 10/027,607 | 12/19/2001 | Kenneth W. Aull | NG(MS)7191 | 3015 |

26294          7590          09/25/2007
TAROLLI, SUNDHEIM, COVELL & TUMMINO L.L.P.
1300 EAST NINTH STREET, SUITE 1700
CLEVEVLAND, OH 44114

| EXAMINER |
|---|
| KHOSHNOODI, NADIA |

| ART UNIT | PAPER NUMBER |
|---|---|
| 2137 | |

| MAIL DATE | DELIVERY MODE |
|---|---|
| 09/25/2007 | PAPER |

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

UNITED STATES PATENT AND TRADEMARK OFFICE

Commissioner for Patents
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450
www.uspto.gov

**MAILED**

SEP 2 5 2007

Technology Center 2100

# BEFORE THE BOARD OF PATENT APPEALS
# AND INTERFERENCES

Application Number: 10/027,607
Filing Date: December 19, 2001
Appellant(s): AULL et al.

Christopher P. Harris
Reg. No. 43,660
<u>For Appellant</u>

**EXAMINER'S ANSWER**

This is in response to the appeal brief filed 6/4/2007 appealing from the Office action

mailed 10/6/2006.

## (1) Real Party in Interest

A statement identifying by name the real party in interest is contained in the brief.

## (2) Related Appeals and Interferences

The examiner is not aware of any related appeals, interferences, or judicial proceedings which will directly affect or be directly affected by or have a bearing on the Board's decision in the pending appeal.

## (3) Status of Claims

The statement of the status of claims contained in the brief is correct, with the exception of claims 1-6, as these claims were cancelled in the After-final amendment filed 10/23/2006.

## (4) Status of Amendments After Final

The appellant's statement of the status of amendments after final rejection contained in the brief is correct.

## (5) Summary of Claimed Subject Matter

The summary of claimed subject matter contained in the brief is correct.

## (6) Grounds of Rejection to be Reviewed on Appeal

The appellant's statement of the grounds of rejection to be reviewed on appeal is correct.

## (7) Claims Appendix

The copy of the appealed claims contained in the Appendix to the brief is correct.

**(8) Evidence Relied Upon**

2003/0005291          Burn                    01-2003

6,490,367             Carlsson et al.         12-2002

**(9) Grounds of Rejection**

The following ground(s) of rejection are applicable to the appealed claims:

*Claim Rejections - 35 USC § 103*

**Claims 1 and 3-20 are rejected under 35 U.S.C. 103(a) as being unpatentable over Burn, United States Pub. No. 2003/0005291 and further in view of Carlsson et al., US Patent No. 6,490,367.**

**As per claim 1:**

Burn substantially teaches a token issuance and binding process comprising: providing a plurality of tokens, each token having a unique ID number stored therein (par. 6, lines 1-7 and par. 37, lines 1-3); generating a unique public/private key pair for each token (par. 36, lines 8-15); storing each token ID number and corresponding public key in a directory/database (par. 36, lines 16-19); storing each private key in its respective token (par. 36-37 and table 1, field name "User Certificate"); and binding a unique ID number of a user to a corresponding one of the plurality of tokens by storing said correspondence there between in the directory/database (par. 36-37 and fig. 5, element 140).

Not explicitly disclosed is reviewing, by a Tokenizing Officer, credentials of the user and forwarding the user ID number and the token ID number to a CMS (Certificate

Management System) along with an E-form (electronic form) request and signature of

the Tokenizing Officer, wherein the Tokenizing Officer comprises a person. However,

Carlsson et al. teach reviewing, by a Tokenizing Officer, credentials of the user and

forwarding the user ID number and the token ID number to a CMS (Certificate

Management System) along with an E-form (electronic form) request and signature of

the Tokenizing Officer, wherein the Tokenizing Officer comprises a person (col. 8, lines

12-51). Therefore, it would have been obvious to a person in the art at the time the

invention was made to modify the method disclosed in Burn to add a Tokenizing Officer,

who is a person, to review credentials of a user and to forward the user information to a

CMS along with an electronic request form and Tokenizing Officer's signature. This

modification would have been obvious because a person having ordinary skill in the art,

at the time the invention was made, would have been motivated to do so since Carlsson

et al. suggest that having a person as the Tokenizing Officer is easy to administer and

adds to security because the credentials are checked by someone who is acquainted

with the users so it is harder to forge an identity in the binding process in col. 8, lines

20-27.

**As per claim 3:**

Burn and Carlsson et al. substantially teach the process as applied to claim 1

above. Not explicitly disclosed is the binding further comprising the CMS checking for

redundant user tokens and revoking any such user tokens. However, Carlsson et al.

teach revoking tokens of individuals when their role has changed in order to do away

with redundant certificates, i.e. so that one user does not have two valid certificates with

different roles especially when one of the roles has been revoked. Therefore, it would

have been obvious to a person in the art at the time the invention was made to modify

the method disclosed in Burn to incorporate the ability to check and revoke any such

tokens that are not distinct.  This modification would have been obvious because a

person having ordinary skill in the art, at the time the invention was made, would have

been motivated to do so since Carlsson et al. suggest that it is important that certificates

that are invalid are revoked in order to prevent from users gaining access to various

objects that they are no longer authorized for in col. 9, lines 14-20.

**As per claim 4:**

Burn and Carlsson et al. substantially teaches the process as applied to claim 3

above.  Furthermore, Carlsson et al. teach the binding further comprising the CMS filling

in the E-form from its directory/database and forwarding the filled in E-form to the

Tokenizing Officer (col. 8, lines 28-37).

**As per claim 5:**

Burn and Carlsson et al. substantially teaches the process as applied to claim 4

above.  Furthermore, Carlsson et al teach the binding further comprising the Tokenizing

Officer reviewing data in filled in E-form and comparing against user credentials and

returning same to CMS after signing (col. 8, lines 12-27).

**As per claim 6:**

Burn and Carlsson et al. substantially teach the process as applied to claim 5

above.   Furthermore, Burn teaches generating and wrapping at least a signature

certificate/private and associated private key for the user in the unique public key of the

token and returning same to the Tokenizing Officer (par. 44, lines 1-13). Not explicitly

disclosed is the binding further comprising the CMS validating the Tokenizing Officer's

signature. However, Burn teaches that when the CA receives a message from the HTP

it must be decrypted, hence verified. Therefore, it would have been obvious to a person

in the art at the time the invention was made to modify the method disclosed in Burn to

incorporate the ability to validate the HTP's signature. This modification would have

been obvious because a person having ordinary skill in the art, at the time the invention

was made, would have been motivated to do so since Burn suggests that validating the

Tokenizing Officer's signature is important to ensure that a valid Tokenizing Officer is

supplying the user information in par. 44, lines 1-5.

**As per claim 7:**

Burn and Carlsson et al. substantially teach the process as applied to claim 6

above. Furthermore, Burn teaches the binding further comprising the Tokenizing Officer

storing the signature certificate/private key for the user in the token (par. 44, lines 14-

21).

**As per claim 8:**

Burn and Carlsson et al. substantially teach the process as applied to claim 7

above. Not explicitly disclosed is the binding further comprising the user unwrapping

the signature certificate/private key using the token private key stored in the token.

However, Burn teaches the HTP unwrapping the signature certificate/private key stored

in the token. Therefore, it would have been obvious to a person in the art at the time the

invention was made to modify the method disclosed in Burn to instead have the user

unwrap the information in the token. This modification would have been obvious

because a person having ordinary skill in the art, at the time the invention was made,

would have been motivated to do so since Burn suggests that in order to use the

certificate it must be able to be decrypted by the private key stored in the token, which is

stored therein to ensure that the private key is kept confidential and will not be

compromised in par. 44, lines 14-21.

**As per claim 9:** ·

Burn and Carlsson et al. substantially teach the process as applied to claim 1

above. Not explicitly disclosed by Burn is the process wherein providing a plurality of

tokens comprises providing a plurality of USB (Universal Serial Bus) tokens. However,

Burn teaches the use of a hardware token that could be implemented in various ways.

Therefore, it would have been obvious to a person in the art at the time the invention

was made to modify the method disclosed in Burn to have the hardware tokens

comprise of USB tokens. This modification would have been obvious because a person

having ordinary skill in the art, at the time the invention was made, would have been

motivated to do so since Burn suggest that any type of hardware token can be used in

par. 46.

**As per claim 10:**

Burn teaches the process as applied to claim 1 above. Not explicitly disclosed by

Burn is the process wherein providing a plurality of tokens comprises providing a

plurality of smart cards. However, Burn teaches that a smartcard could be used in an

alternate embodiment. Therefore, it would have been obvious to a person in the art at

the time the invention was made to modify the method disclosed in Burn to have the

hardware tokens comprise of smartcards. This modification would have been obvious

because a person having ordinary skill in the art, at the time the invention was made,

would have been motivated to do so since Burn suggests that any type of hardware

token can be used, for example a smart card, in par. 31.

**As per claim 11:**

**The limitations in claim 11 are similar in scope to the limitations disclosed**

**in claim 1, thus it is rejected for the same reasons since it is merely the system**

**that implements the rejected method claim.**

**As per claims 12-20:**

**The limitations in claims 12-20 are similar in scope to the limitations**

**disclosed in claims 3-10, thus it are rejected for the same reasons since they are**

**merely components of the system that implement the rejected method claims.**


**(10) Response to Argument**

**Regarding Claim 1:**

Appellant contends that "Burn taken in view of Carlsson does not teach or

suggest reviewing, by a Tokenizing Officer, credentials of a user and forwarding a user

ID number and a token ID number to a CMS along with an electronic form request and a

signature of the Tokenizing Officer, as recited in claim 1." Examiner respectfully

disagrees. Examiner would first like to note that Burn teaches: a unique ID number

stored in the token (Fig. 5, element 140: "*USER PIN*" and par. 36, line 6-8: "*In steps 85*

*and 90, personal identification numbers (PINs) are randomly generated.*"); a

unique public/private key pair generated, where the private key is stored in the token

(Fig. 4, element 115: "*STORE USER CERTIFICATE IN HTP*" and par. 36, lines 8-13,

where the 'public key' is the "*certification number*" and the 'private key' is the "*user

certificate*"); a token ID number (Fig. 5, element 130: "*HTP ID #*") stored with the public

key (Fig. 5, element 160: "*USER CERTIFICATION NUMBER*") in a database (Fig. 5,

title: "*HTP RECOGNITION TABLE*" described in paragraph 38); and finally, where the

unique ID number of a user (i.e. the user ID number) is bound to one of a plurality of

tokens by storing a correspondence between the two in the directory/database (Fig. 5,

elements 130: "*HTP ID #*" and 140: "*USER PIN*"). It is also important to note that Burns

teaches an enrollment phase wherein all of the above elements are stored in a

recognition database in order to register the user as an authenticated user as specified

in paragraph 47, lines 13-17: "*Also using distinct certificates helps to ensure that

the HTP engaged in enrollment is the correct HTP* and that no other HTP can

inadvertently receive user-specific certificates that are encrypted with a distinct non-user

specific certificate.*" Thus, Burn teaches that in order to bind the user to a particular

HTP (i.e. token), the user must be properly enrolled via a certificate authority using the

information from the HTP, in addition to user data in paragraph 41, lines 1-8: "*FIG. 7 is a

flow diagram that depicts the HTP enrollment process. Once HTPs are initialized, they

are distributed to potential new users. Once a user obtains an HTP, that user must

engage in an enrollment process that result of which affiliates that user with a

particular HTP.* Using the user's own workstation, or any other workstation augmented

*with an HTP reader 50, **the user must send an enrollment request to the certificate**

**authority** (step 220)."* Burn was modified by Carlsson et al. since Carlsson et al.

specifically mentioned the use of a method which has a Tokenizing Officer, who is a

person, validate the user's credentials, then signs and forward those credentials to the

Certificate Management System (i.e. CA center) in col. 8, lines 20-37: **"The CA**

**administrator checks that the user is entitled to certification and verifies the**

**user's identity. One of the advantages of the distributed CA architecture is that**

**this stage is easy to administer in a satisfactory manner as regards security. The**

**CA administrator may be reasonably familiar with the users he is to certify, since**

**he/she works with them on a daily basis. The administrator then uses the CA**

**terminal to complete a form with the user information and validity periods which**

**are required in order to create a certificate.** *The CA terminal checks the plausibility*

*of the input information and generates an RSA key pair (keys may optionally be*

*generated in the CA terminal, in the CA centre, in the administrator's card or in the*

*user's card).* **Before certificate data is sent to the CA centre, the certification data**

**is signed, together with the service life and sequence number of the certificate**

**request, by the administrator (using the administrator's card)."** Carlsson et al. thus

modifies Burn to not only incorporate a Tokenizing Officer as a middle-man to validate a

user's credentials via direct contact, but then forwards the credentials (as disclosed in

Burn), which are signed and verified by this Tokenizing Officer to add a level of security

in authenticating the user. Carlsson et al. mentions that verifying the user's identity

before allowing for the assignment of a certificate is necessary in order to ensure that

only valid users are assigned credentials such as public/private keys and a certificate.

Thus, using the information mentioned by Carlsson et al. in combination with the Burn

yields the limitation presented in claim 1. Specifically, Burn teaches sending credentials

to a CA (where these credentials include information regarding the specific HTP, i.e.

token ID number, and user information, i.e. user PIN, in order to bind the user and token

together with a certificate that is issued to the user. So, taking that in combination with

Carlsson's Tokenizing Officer verifying the user's identity in person and sending the

user ID and a sequence number for the certificate (which could be replaced with the

token ID number taught in Burn), yields a secure system of authenticating and validating

user's before binding their identity to a certificate and a hardware token. The motivation

for this combination as provided by Carlsson et al., is that having a person as the

Tokenizing Officer is easy to administer and adds to security because the credentials

are checked by someone who is acquainted with the users so it is harder to forge an

identity in the binding process. Therefore, Burn taken in view of Carlsson does

teach/suggest reviewing, by a Tokenizing Officer, credentials of a user and forwarding a

user ID number and a token ID number to a CMS along with an electronic form request

and a signature of the Tokenizing Officer, as recited in claim 1.

Finally, Examiner would like to note that the test for obviousness is not whether

the features of a secondary/tertiary reference(s) may be bodily incorporated into the

structure of the primary reference; nor is it that the claimed invention must be expressly

suggested in any one or all of the references. Rather, the test is what the combined

teachings of the references would have suggested to those of ordinary skill in the art.

See *In re Keller*, 642 F.2d 413, 208 USPQ 871 (CCPA 1981).

**Regarding Claim 3:**

Appellant contends, "Burn taken in view of Carlsson does not teach or suggest a

CMS checking for redundant user tokens and revoking any such user tokens."

Examiner respectfully disagrees. Burn teaches that an enrollment process is necessary

in order to maintain a system where each HTP is associated with one user in paragraph

47, lines 13-17: "***Also using distinct certificates helps to ensure that the HTP***

***engaged in enrollment is the correct HTP and that no other HTP can inadvertently***

***receive user-specific certificates that are encrypted with a distinct non-user***

***specific certificate.***" Burn also teaches the use of a flag to show whether or not the

HTP has been initialized with the elements disclosed above (Fig. 5, element 145:

"***INITIALIZED***" and page. 4, "Table 1-continued": row for "Initialized"). Carlsson et al. is

used to modify Burn since Carlsson et al. go into more specific detail regarding

revocation. Specifically, Carlsson et al. teach that a CA administrator manages user

cards and has the ability to revoke a card, i.e. token, if a circumstance necessitating that

revocation occurs in col. 7, lines 65-67: "*In addition,* ***the administrator will make the***

***cards unusable (destroy them) when the stored certificate is revoked.***" Carlsson et

al. also suggest that certificates are revoked for various reasons, including that a certain

role is no longer available to a user in order to do away with redundant certificates per

user in col. 9, lines 14-20: "***A certificate is revoked (=declared invalid) when the***

***certificate has become invalidated for some reason.*** *This can occur, for example*

*when a user has dies,* **has been found to be unreliable, or his/her role has changed.**
*Before the CA administrator revokes a user's certificate, a check will be made according*
*to the administrative rules of the organization."* Thus, based on the previous two

passages cited, a certificate may be revoked when a user's role changes in order to

prevent from one user being authorized to do several tasks (some of which have been

completed) at one time or is deemed unreliable, where a token may be

revoked/destroyed for any of the above reasons. Carlsson et al. further suggest various

other administration tasks which a CA administrator is responsible for carrying out,

including the prevention of unauthorized users gaining access to tokens not assigned to

them (col. 17, lines 7-35). Thus, it would have been obvious to modify the method

disclosed by Burn and Carlsson et al. from claim 1 to incorporate a means of checking

the token ID number and flags of the tokens (disclosed in Burn) against other tokens

and revoking tokens which are no longer valid since the user's certificate has been

revoked (disclosed in Carlsson et al.). One would been motivated to modify the method

disclosed since Carlsson et al. suggest that it is important that certificates that are

invalid are revoked in order to prevent from users gaining access to various objects that

they are no longer authorized for in col. 9, lines 14-20. Thus, Burn taken in view of

Carlsson does teach/suggest a CMS checking for redundant user tokens and revoking

any such user tokens.

**Regarding Claim 11:**

Appellant contends that "Burn taken in view of Carlsson does not teach or

suggest reviewing, by a Tokenizing Officer, credentials of a user and forwarding a user

ID number and a token ID number to a CMS along with an electronic form request and a

signature of the Tokenizing Officer, as recited in claim 11." Examiner respectfully

disagrees. Examiner would first like to note that Burn teaches: a unique ID number

stored in the token (Fig. 5, element 140: "*USER PIN*" and par. 36, line 6-8: "*In steps 85*

*and 90, personal identification numbers (PINs) are randomly generated.*"); a

unique public/private key pair generated, where the private key is stored in the token

(Fig. 4, element 115: "*STORE USER CERTIFICATE IN HTP*" and par. 36, lines 8-13,

where the 'public key' is the "*certification number*" and the 'private key' is the "*user*

*certificate*"); a token ID number (Fig. 5, element 130: "*HTP ID #*") stored with the public

key (Fig. 5, element 160: "*USER CERTIFICATION NUMBER*") in a database (Fig. 5,

title: "*HTP RECOGNITION TABLE*" described in paragraph 38); and finally, where the

unique ID number of a user (i.e. the user ID number) is bound to one of a plurality of

tokens by storing a correspondence between the two in the directory/database (Fig. 5,

elements 130: "*HTP ID #*" and 140: "*USER PIN*"). It is also important to note that Burns

teaches an enrollment phase wherein all of the above elements are stored in a

recognition database in order to register the user as an authenticated user as specified

in paragraph 47, lines 13-17: "*Also using distinct certificates helps to ensure that*

*the HTP engaged in enrollment is the correct HTP and that no other HTP can*

*inadvertently receive user-specific certificates that are encrypted with a distinct non-user*

*specific certificate.*" Thus, Burn teaches that in order to bind the user to a particular

HTP (i.e. token), the user must be properly enrolled via a certificate authority using the

information from the HTP, in addition to user data in paragraph 41, lines 1-8: "*FIG. 7 is a*

flow diagram that depicts the HTP enrollment process. Once HTPs are initialized, they

are distributed to potential new users. **Once a user obtains an HTP, that user must**

**engage in an enrollment process that result of which affiliates that user with a**

**particular HTP.** Using the user's own workstation, or any other workstation augmented

with an HTP reader 50, **the user must send an enrollment request to the certificate**

**authority** (step 220)." Burn was modified by Carlsson et al. since Carlsson et al.

specifically mentioned the use of a system which has a Tokenizing Officer, who is a

person, validate the user's credentials, then signs and forward those credentials to the

Certificate Management System (i.e. CA center) in col. 8, lines 20-37: "**The CA**

**administrator checks that the user is entitled to certification and verifies the**

**user's identity. One of the advantages of the distributed CA architecture is that**

**this stage is easy to administer in a satisfactory manner as regards security. The**

**CA administrator may be reasonably familiar with the users he is to certify, since**

**he/she works with them on a daily basis. The administrator then uses the CA**

**terminal to complete a form with the user information and validity periods which**

**are required in order to create a certificate.** The CA terminal checks the plausibility

of the input information and generates an RSA key pair (keys may optionally be

generated in the CA terminal, in the CA centre, in the administrator's card or in the

user's card). **Before certificate data is sent to the CA centre, the certification data**

**is signed, together with the service life and sequence number of the certificate**

**request, by the administrator (using the administrator's card).**" Carlsson et al. thus

modifies Burn to not only incorporate a Tokenizing Officer as a middle-man to validate a

user's credentials via direct contact, but then forwards the credentials (as disclosed in

Burn), which are signed and verified by this Tokenizing Officer to add a level of security

in authenticating the user. Carlsson et al. mentions that verifying the user's identity

before allowing for the assignment of a certificate is necessary in order to ensure that

only valid users are assigned credentials such as public/private keys and a certificate.

Thus, using the information mentioned by Carlsson et al. in combination with the Burn

yields the limitation presented in claim 11. Specifically, Burn teaches sending

credentials to a CA (where these credentials include information regarding the specific

HTP, i.e. token ID number, and user information, i.e. user PIN, in order to bind the user

and token together with a certificate that is issued to the user. So, taking that in

combination with Carlsson's Tokenizing Officer verifying the user's identity in person

and sending the user ID and a sequence number for the certificate (which could be

replaced with the token ID number taught in Burn), yields a secure system of

authenticating and validating user's before binding their identity to a certificate and a

hardware token. The motivation for this combination as provided by Carlsson et al., is

that having a person as the Tokenizing Officer is easy to administer and adds to

security because the credentials are checked by someone who is acquainted with the

users so it is harder to forge an identity in the binding process. Therefore, Burn taken in

view of Carlsson does teach/suggest reviewing, by a Tokenizing Officer, credentials of a

user and forwarding a user ID number and a token ID number to a CMS along with an

electronic form request and a signature of the Tokenizing Officer, as recited in claim 11.

Finally, Examiner would like to note that the test for obviousness is not whether

the features of a secondary/tertiary reference(s) may be bodily incorporated into the

structure of the primary reference; nor is it that the claimed invention must be expressly

suggested in any one or all of the references. Rather, the test is what the combined

teachings of the references would have suggested to those of ordinary skill in the art.

See *In re Keller*, 642 F.2d 413, 208 USPQ 871 (CCPA 1981).

**Regarding Claim 13:**

Appellant contends, "Burn taken in view of Carlsson does not teach or suggest

that a user cannot possess more than one personalized card (e.g. token)." Examiner

respectfully disagrees. Burn teaches that an enrollment process is necessary in order to

maintain a system where each HTP is associated with one user in paragraph 47, lines

13-17: "***Also using distinct certificates helps to ensure that the HTP engaged in***

***enrollment is the correct HTP and that no other HTP can inadvertently receive***

***user-specific certificates that are encrypted with a distinct non-user specific***

***certificate.***" Burn also teaches the use of a flag to show whether or not the HTP has

been initialized with the elements disclosed above (Fig. 5, element 145: "*INITIALIZED*"

and page. 4, "Table 1-continued": row for "Initialized"). Carlsson et al. is used to modify

Burn since Carlsson et al. go into more specific detail regarding revocation.

Specifically, Carlsson et al. teach that a CA administrator manages user cards and has

the ability to revoke a card, i.e. token, if a circumstance necessitating that revocation

occurs in col. 7, lines 65-67: "*In addition, **the administrator will make the cards***

***unusable (destroy them) when the stored certificate is revoked.***" Carlsson et al.

also suggest that certificates are revoked for various reasons, including that a certain

role is no longer available to a user in order to do away with redundant certificates per

user in col. 9, lines 14-20: "**A certificate is revoked (=declared invalid) when the**

**certificate has become invalidated for some reason.** This can occur, for example

when a user has dies, **has been found to be unreliable, or his/her role has changed.**

Before the CA administrator revokes a user's certificate, a check will be made according

to the administrative rules of the organization." Thus, based on the previous two

passages cited, a certificate may be revoked when a user's role changes in order to

prevent from one user being authorized to do several tasks (some of which have been

completed) at one time or is deemed unreliable, where a token may be

revoked/destroyed for any of the above reasons. Carlsson et al. further suggest various

other administration tasks which a CA administrator is responsible for carrying out,

including the prevention of unauthorized users gaining access to tokens not assigned to

them (col. 17, lines 7-35). Thus, it would have been obvious to modify the system

disclosed by Burn and Carlsson et al. from claim 12 to incorporate a means of checking

the token ID number and flags of the tokens (disclosed in Burn) against other tokens

and revoking tokens which are no longer valid since the user's certificate has been

revoked (disclosed in Carlsson et al.). One would been motivated to modify the system

disclosed since Carlsson et al. suggest that it is important that certificates that are

invalid are revoked in order to prevent from users gaining access to various objects that

they are no longer authorized for in col. 9, lines 14-20. Thus, Burn taken in view of

Carlsson does teach/suggest a CMS checking for redundant user tokens and revoking

any such user tokens.


## (11) Related Proceeding(s) Appendix

No decision rendered by a court or the Board is identified by the examiner in the

Related Appeals and Interferences section of this examiner's answer.


For the above reasons, it is believed that the rejections should be sustained.

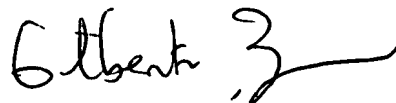Respectfully submitted,

Nadia Khoshnoodi

GILBERTO BARRON JR
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100

Conferees

Gilberto Barron


Matthew Smithers                         /Matthew Smithers/
                                         Primary Examiner, Art Unit 2137